REMARKS/ARGUMENTS

Claims 1 to 33 are currently pending in the application. The Examiner has objected to the specification due to the use of widely understood acronyms. The Examiner has also objected to claim 17 as allegedly including an informality. The Examiner has rejected claims 1-3, 8-10, 12-16, 20 and 26 under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 6,046,980 to Packer. Claims 6, 7, 17, 21, 22 and 25 have been rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 6,144,636 to Aimoto et al. Claims 11, 18, 19, 23, 24, 27-33 have been rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 6,122,670 to Bennett. Claims 3 to 5 have been rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Packer in view of Bennett.

In response to the Examiner's objection to the specification, Applicant has amended the specification to insert, at their respective first occurrences in the specification, the full names for the acronyms TCP, IP, HTTP, WAN, FTP, and MIME. The Examiner appears to require replacing each occurrence of the foregoing acronyms with the corresponding full name. However, this does not appear to be required by any applicable rule or statute. Applicant submits that spelling out the full name at the first occurrence of each acronym followed by the acronym itself is more than sufficient.

The Prior Art Rejections

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." See MPEP § 2131 (quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The U.S. Patent and Trademark Office has just recently issued new guidelines for determining obviousness under 35 U.S.C. § 103 in view of the Supreme Court's decision in KSR Int'l Co. v. Teleflex Inc. See Federal Register/Vol. 72, No. 195 at 57526. Consistent with past practice, however, the guidelines still require Examiners, when basing rejections on the

combination of prior art, to articulate either 1) "a finding that the prior art included each element claimed," see Federal Register/Vol. 72, No. 195 at 57529; or 2) "a finding that there was some teaching, suggestion, or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." See Federal Register/Vol. 72, No. 195 at 57534.

Claims 1, 17 to 19, 21 and 26

Claim 1 is directed to using behavioral models of network applications to classify network traffic. Similarly, claims 17 to 19 are directed to methods that model the behavior of a network application and using the modeled behavior to classify network traffic. The behavior pattern includes at least one instance of a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows. Claim 21 is directed to an apparatus that classifies data flows based on observed behavior, as well as explicitly-presented packet attributes. Claim 21 has also been amended to further define application behavior pattern to include one or more of "a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet timing value, a sequence of protocol flags, or an inter-packet protocol flag timing value." Claim 26 has similar limitations to claim 21.

Packer fails to anticipate the subject matter of claims 1, 21 and 26. Packer, like the prior art discussed in the background section of the present application, classifies network traffic based on inspection of explicitly presented attributes of packets in the data flows, such as protocol identifiers and the like. Claim 1, on the other hand, utilizes a knowledge base of known application behavior patterns to classify network traffic. The dependent claims, and the discussion that follows, present examples of application behavior patterns. As to claims 21 and 26, Packer fails to disclose or suggest a system that classifies network traffic based on application behavior patterns and explicitly-presented packet attributes. Further, as to claims 21 and 26, Packer fails to teach an application behavior pattern that includes one or more of "a packet size pattern, a threshold information density value, a threshold inter-flow timing value, or a threshold number of related application data flows, an inter-packet timing value, a sequence

of protocol flags, or an inter-packet protocol flag timing value."

The Examiner's reliance on Aimoto is misplaced to reject claims 17 and 19. Aimoto is directed to a network switch with a congestion control function. The metrics monitored by Aimoto such as cell count, bit rate, and the like are monitored relative to respective traffic classes. Aimoto, however, does not use such metrics to actually classify the network traffic. Rather, Aimoto uses the standard paradigm to classify network traffic. That is, the network switch of Aimoto uses explicitly presented attributes of the cells (here, Switched of Permanent Virtual Connection identifiers—termed "VCIs" in Aimoto) to associate the cells with a traffic class. The metrics maintained by Aimoto are used to control congestion, not classify traffic.

Claims 2-5

Claims 2 to 5 are directed to the classification of data flows based on a behavior pattern that considers the sizes of packets.

As to claim 2, the Examiner alleges that Packer teaches classification of a data flow based on the packet size of a packet in the data flow. This allegation is plainly unsupportable. For example, the Examiner points to Table 2 of Packer (Col. 12). Table 2 of Packer merely depicts some of the attributes that may be used to classify network traffic. None of these attributes, however, are directed to the size of the packets of a data flow. Indeed, Packer is devoid of any teaching that discloses or suggests consideration of packet size or patterns that include packet size in the classification of data flows.

The Examiner appears to allege that the combination of Bennett and Packer teaches the subject matter of claims 3 to 5. Again, this contention is unsupportable. The Examiner's reliance of the fragmentation processes disclosed in Bennett is completely misplaced and not well taken. Bennett appears to describe a system that offloads reliable communications protocol processing (such as TCP) to hardware. Bennett, Col. 1, line 57 to Col. 2, line 9; Col. 3, lines 46-57. Indeed, the passage quoted in the office action at page 21 fails to teach the claimed subject matter. The quoted passage is directed to receiving a packet and computing a checksum as a lookup to identify other packets that may have been accumulated according to a defragmentation process. Nothing in Bennett, however, teaches classification of data flows

based on behavior patterns that consider the sizes of packets of a data flow.

Claims 6 and 7

Claims 6 and 7 are directed to a traffic classification system that uses a behavior pattern that considers the information density of respective packets.

The Examiner appears to allege that Aimoto anticipates the subject matter of claims 6 and 7. Again, the Examiner's reliance on Aimoto is completely misplaced. Aimoto merely describes a packet switching function that addresses network congestion. The passage of Aimoto cited by the Examiner teaches the use of a packet buffer shared by a plurality of output ports. For each traffic class, a counter is maintained. A congestion notification is generated when a threshold cell count number is exceeded. Aimoto, Col. 3, lines 7-22. The Examiner appears to allege that a threshold relating to the number of cells buffered for a given traffic class is equivalent to the "information density" of a packet. Information density is disclosed at paragraph 0051 of Applicant's specification. Information density characterizes the level of randomness in the data of a given packet. Accordingly, the Examiner appears to incorrectly equate a congestion threshold based on the number of packets stored in a buffer with a metric that characterizes the density of information of a packet. Still further, the Examiner's rejection is also improper because the Examiner fails to consider that, even assuming Aimoto teaches the concept of information density, Aimoto does not teach the use of information density to classify data flows.

Claims 8 and 9

Claims 8 and 9 are directed to a traffic classification system that uses a behavior pattern that considers the presence of other, similar data flows associated with the same host. Claim 8 involves an evaluation of the timing of these related flows, while claim 9 involves evaluation of the number of related flows. Paragraphs 0052 and 0053 of the specification teach this subject matter.

The Examiner incorrectly alleges that Packer discloses the subject matter of claims 8 and 9. The passage of Packer (Col. 10, lines 32-42) merely discloses the detection of a data rate based

on the timing of when a packets of a data flow are received. Accordingly, the Examiner's rejection is incorrect for two reasons. First, Packer does not disclose consideration of the timing or number of related or similar flows associated with a host. Second, Packer fails to disclose consideration of the timing or number of related or similar flows associated with a host for the purposes of classifying a data flow.

Claims 10 to 16, and 20

Claims 10 to 16 are directed to a traffic classification system that uses a behavior pattern that considers the timing of various events associated with a data flow, such as the timing between two packets of a flow, the timing and sequence of protocol flags and the like. Similarly, claim 20 is directed to matching a data flow to a traffic class, if a threshold number of data flows of the host match a corresponding behavior model.

As to claims 10 to 16 and 20, the Examiner's reliance on Packer is fatally defective. The common error across the Examiner's rejections is the recital of some disclosed function in Packer, such as examination of data rate, without any support in Packer that the recited function is used in a behavior pattern against which data flows may be classified. For example, as to claim 20, nowhere does Packer teach the classification of a data flow based on the number of other data flows associated with a given host that also match a behavior pattern. Furthermore, as to claim 10, while Packer discloses identification of a data rate, it does not disclose use of a data rate to classify network traffic.

Claims 29 to 31

Claims 29 and 31 have been amended such that they are directed to the classification of network traffic based on the computed entropy of information contained in packets of a data flow.

As discussed above, neither Bennett nor Aimoto, disclose the classification of network traffic based on entropy or information density of packets of a data flow. Aimoto has been discussed above in connection with claims 6 and 7. Bennett merely computes checksums of IP addresses or other headers to match packets that have been buffered as part of a

defragmentation process. As discussed, Bennett does not teach the application of an entropy or information density function to classify data flows.

Claim 33

Lastly, claim 33 has been amended to clarify that the received packets of a data flow have respective first checksums, and that classification is based on computing second checksums and comparing the second checksums to the first checksums contained in the packets.

The Examiner's reliance of the fragmentation processes disclosed in Bennett is again misplaced. The quoted passages of Bennett teach to receiving a packet and computing a checksum as a lookup to identify other packets that may have been accumulated according to a defragmentation process. Nothing in Bennett, however, teaches classification of data flows based on behavior patterns that consider whether the computed second checksum should match the checksum contained in received packets. Indeed, checksums are generally used to check for transmission errors. The claimed subject matter is a novel use of checksums to classify network traffic based on the existence of some network applications that intentionally include incorrect checksums. See Specification at ¶ 0056.

In light of the foregoing, Applicant believes that all currently pending claims are presently in condition for allowance. Applicant respectfully requests a timely Notice of Allowance be issued in this case. If the Examiner believes that any further action by Applicant is necessary to place this application in condition for allowance, Applicant requests a telephone conference with the undersigned at the telephone number set forth below.

Respectfully Submitted,
LAW OFFICE OF MARK J. SPOLYAR

/Mark J. Spolyar/
Mark J. Spolyar
Reg. No. 42,164

Date: January 2, 2008
Customer Number: 30505
Law Office of Mark J. Spolyar
2200 Cesar Chavez St, Suite 8
San Francisco, CA 94124
415-826-7966
415-480-1780 fax